Twisted Edwards curve and its group of points over finite field $F_p$

U. V. Skrunkovich  
NTUU, Kiev, Ukraine  
 julian.skrunkovich@gmail.com  

R. V. Skuratovskii  
NPU, Kiev, Ukraine  
ruslan@imath.kiev.ua

We consider the conditions of supersingularity of Edwards curve [1–3]. A normalization of this curve was constructed by us in projective form. We denote twisted Edwards curve having coefficients $a$ and $d$ as $E_{a,d}$. It was found the mistake in conditions of supersingularity for this curve in theorem 3 of article [4]. More particularly if $p \equiv -3 (mod 8)$ there is no degenerated twisted pair of curves as it states in [4]. Also if condition $p \equiv \pm 7 (mod 8)$ holds then the orders of correspondent curves are such $N_{E_2} = N_{E_{2-1}} = p - 3$ that are not equal $p + 1$ as it states in [4]. For instance if $p = 31$ then $N_{E_2} = N_{E_{2-1}} = 28 = 8 \cdot 3 + 7 - 3$.

The main result of this paper is the theorem.

**Theorem 1.** If $p \equiv 3 (mod 4)$ and $p$ is prime, then numbers of points on $x^2 + y^2 = 1 + 2x^2y^2$ and on $x^2 + y^2 = 1 + 2^{-1}x^2y^2$ over $F_p$ are equal $N_{E_{1,2}} = N_{E_{1,2-1}} = p + 1$ when $p \equiv 3 (mod 8)$ and $N_{E_2} = N_{E_{2-1}} = p - 3$ when $p \equiv 7 (mod 8)$.

There are two fundamental points [6] $((0, \pm 1), (\pm \sqrt{a}, 0))$ on $E_{a,d}$. The interesting relations between points of $E_{a,d}$ were found.

**Theorem 2.** For every no fundamental point $(x, y)$ of $E_{a,d}$ holds the condition $\left(\frac{1-ax^2}{p}\right) \left(\frac{1-y^2}{p}\right) = \left(\frac{a-d}{p}\right)$.

If $a$ is a quadratic residue over $F_p$ then it exists the isomorphism between Edwards curve $E_{1,d}$ and twisted Edwards curve $E_{a,d}$, which is given by the mapping $X \mapsto \sqrt{a}x, Y \mapsto y$. This fact and the theorem 1 lead us to a condition of supersingularity of $E_{a,d}$.

**Remark.** Point of order 8 exists on $E_{a,d}$ if and only if point of order 4 exists on $E_{a,d}$ and following conditions holds $\left(\frac{2(1\pm \sqrt{p-2})}{p}\right) = 1$, $\left(\frac{2(1\pm \sqrt{p-2})}{p}\right) = 1$, $\left(\frac{2}{p}\right) = 1$, $\left(\frac{2}{p}\right) = 1$.

**References**


